

Application No. 10/044,242

2

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of the Claims:

- 1 1. (currently amended) A system for managing volatile storage of information
2 for operating a device having extended periods of inactivity between periods
3 of activity comprising:
4 volatile memory connected to receive said information from a
5 source and enabled to retain said information during power-on conditions;
6 processing circuitry coupled to said volatile memory to process
7 said information during said periods of activity; [[and]]
8 a volatile memory checker enabled to execute between said
9 periods of activity, said volatile memory checker including test code
10 configured to detect soft errors within said information retained in said volatile
11 memory, said volatile memory being susceptible to soft errors; and
12 said soft errors detected via execution of said volatile memory
13 checker being soft errors occurring during said extended periods of inactivity
14 between said periods of activity of said device.
- 1 2. (original) The system of claim 1 wherein said volatile memory, said
2 processing circuitry and said volatile memory checker are integrated into a
3 single integrated circuit chip, said test code being configured to detect soft
4 errors.
- 1 3. (original) The system of claim 2 wherein said volatile memory is one or
2 both of dynamic random access memory (DRAM) and static random access
3 memory (SRAM) embedded within said integrated circuit chip, said
4 processing circuitry including a processing unit.

Application No. 10/044,242

3

1 4. (original) The system of claim 1 wherein said volatile memory checker
2 includes a timing module enabled to trigger execution of said test code in
3 response to detection of a passage of a preselected time period and
4 simultaneous detection that said device is in a period of inactivity.

1 5. (original) The system of claim 1 further comprising a recovery module
2 responsive to said volatile memory checker to selectively trigger information
3 replacement for said volatile memory upon detecting said errors, said
4 information being executable code for operating said device.

1 6. (original) The system of claim 5 wherein said recovery module is
2 configured to selectively reinitialize said device to initiate a transfer of said
3 executable code from said source to said volatile memory.

1 7. (original) The system of claim 5 wherein said recovery module is
2 configured to selectively reset said device in response to a system-wide error
3 in execution of said executable code.

1 8. (original) The system of claim 5 wherein said volatile memory checker is
2 configured to perform a cyclic redundancy check (CRC) or checksum of
3 executable code memory space of said volatile memory.

1 9. (original) The system of claim 1 wherein said volatile memory, said
2 processing circuitry and said volatile memory checker are integrated into an
3 application specific integrated circuit (ASIC) of a printer controller.

1 10. (original) The system of claim 1 wherein said volatile memory and said
2 processing circuitry are housed within separate integrated circuit chips.

Application No. 10/044,242

4

1 11. (currently amended) A method of assessing integrity of executable code
2 comprising the steps of:
3 transferring said executable code into volatile memory of a
4 device that is activated upon execution of said executable code, said device
5 being in an inactive state between executions of said executable code;
6 performing time-based volatile memory checking routines in
7 response to detecting that said device is in said inactive state and a
8 preselected time period has elapsed, including checking code space of said
9 volatile memory to detect soft errors within said executable code, said volatile
10 memory being susceptible to said soft errors, wherein said soft errors are
11 those errors occurring within said executable code during said inactive state
12 between said executions of said executable code; and
13 initiating a selected response upon detecting fatal code error
14 during performing said checking routines.

1 12. (original) The method of claim 11 wherein said step of performing said
2 routines includes calculating a cyclic redundancy check (CRC) or checksum
3 for executable code space of said volatile memory.

1 13. (original) The method of claim 11 wherein said step of initiating said
2 selected response includes triggering a reinitialization that repeats said step
3 of transferring said executable code into said volatile memory.

1 14. (original) The method of claim 13 wherein said step of initiating further
2 includes resetting said device in response to a code error that results in said
3 checking routines being terminated.

1 15. (original) The method of claim 11 wherein said step of transferring
2 includes loading said executable code into random access memory
3 embedded in an integrated circuit having a central processor.

Application No. 10/044,242

5

1 16. (original) The method of claim 15 wherein said step of performing said
2 checking routines includes scheduling said checking routines to occur on a
3 periodic basis.

1 17. (original) An integrated circuit comprising:
2 a processor;
3 embedded volatile memory having an input to receive
4 executable code that includes instructions specific to operations of said
5 processor;
6 an integrated self-tester having stored test code specific to
7 detecting code error in said executable code during storage in said volatile
8 memory, said self-tester being responsive to a time-based test initialization
9 signal for triggering periodic testing; and
10 a recovery module responsive to said self-tester to induce an
11 operational sequence that transfers fresh executable code to said input of
12 said volatile memory when said self-tester detects a specific code error
13 condition.

1 18. (original) The integrated circuit of claim 17 wherein said volatile memory
2 is one or both of dynamic random access memory (DRAM) and static random
3 access memory (SRAM), said specific code error condition including alpha
4 particle-induced error detections that are pre-identified as being fault
5 conditions.

1 19. (original) The integrated circuit of claim 17 wherein said self-tester
2 includes embedded non-volatile memory for storing said test code.

1 20. (original) The integrated circuit of claim 17 wherein said processor and
2 said executable code are specific to operating within a printer controller.

1 21. (original) The integrated circuit of claim 17 wherein said recovery module
2 includes code for inducing reinitialization in which said volatile memory is
3 reloaded with said executable code from a source of said executable code.

Application No. 10/044,242

6

1 22. (currently amended) A system for managing information storage
2 comprising the steps of:
3 storing said information within memory that is susceptible to
4 occurrences of soft errors, said memory being within a device that is
5 characterized by extended periods of inactivity between periods of activity;
6 processing circuitry coupled to said memory to process said
7 information during said periods of activity; and
8 an automated memory checker enabled to execute between
9 said periods of activity, said automated memory checker being configured to
10 execute test code on a timed basis to detect said soft errors within said
11 information stored in said memory, said soft errors of interest being those
12 errors occurring during said extended periods of inactivity between said
13 periods of activity.

1 23. (original) The system of claim 22 wherein storing said information in
2 memory includes magnetically recording said information on a medium
3 susceptible to said occurrences of soft errors.

1 24. (original) The system of claim 22 wherein storing said information
2 includes embedding said information within non-volatile memory housed
3 within an integrated circuit chip, wherein said non-volatile memory is
4 susceptible to said occurrences of soft errors.